CIO SECURITY COUNCIL COMMITTEE MINUTES
January 10, 2007

Checklist for reporting and collecting data regarding misuse of state equipment

- Lesa Quinn reported: Contact was made with the DCI in regard to internet, inappropriate use, etc. One of the suggestions from the DCI was to contact local law enforcement for criminal charges
- Missouri has actual state statutes and Administrative Rules and Lesa is researching
- Not a lot of information exists out there for checklists; more research needs to be done and a checklist created
- It would be helpful for IT staff to know what logs to look at; what each step is along the way to conduct forensics testing
- Some departments would rather conduct the investigation themselves rather than turn it over to another agency
- Greg Fay reported: ISO (Information Security Office) – just a reminder the ISO is anxious to assist; they have some tools to assist in the forensics testing, although not as in-depth as the DCI; however, they can look at machines to see if they have been used for inappropriate use
- Lesa Quinn reminded members that we did discuss an acceptable use policy at our November meeting. She had three policies submitted to her; as soon as hers is done, she will then post all of them on the ISO site so other agencies can use them as examples. Currently their acceptable use policy is being reviewed by the JAG. She will see if she can get the Guard or DOD acceptable use policy.
- As a reminder, acceptable use policy will cover hardware. There was some discussion whether the DAS acceptable use policy covers personal equipment brought from home. One interpretation is that if an employee brings a piece of equipment from home and uses it on the state network, then it becomes state-owned equipment.
- Some consider this to be a training issue if it is adopted. Employees will have to be told what the expectation is.
- Dept of Revenue now has tracking software. They can track who puts USBs on the network, etc. The day the software was installed, they were able to identify an employee who was moving a significant amount of data to an external device.

Network access control – where are we going to get the money to implement this?

Cyber Security Exercise Project

- We need volunteers for this project to work on a committee. We need to proceed with regular exercises. ISO offered to coordinate the project and will be getting started with the planning phase soon. Since the meeting a committee has been formed. Greg Fay, Bill Hubbard, Deb Castillo, Shane Ludwig and Barnard Gaumer. Assistance from Homeland Security Bret Voorhees and Lesa Quinn will help facilitate.

Technology Customer Council Committee – members of the state CIO Security council were brought up to date on the latest meeting with the Technology Customer Council.

- There was discussion with the committee regarding the utility and the money from the unfilled position in the security office and ways to maximize those dollars for current needs;
- An enterprise-wide security exercise. Need to make good use of the utility to coordinate the exercise; it doesn't need to be terribly complex
- The key issue is if we have an incident we need to have, at a minimum, contact phone numbers
- The exercise needs to be a meaningful scenario with effective communications
- Agencies need to follow their COOP/COG plan
- Discussions with the committee have been effective to help with the standards
- In the next week or 2, possible scenarios will be sent out to the committee; need to discuss how this might be put together and things we can do to make it more effective
- It is anticipated that it will be a two-hour exercise
    - Lesa would like to do it at the EOC – so we can really understand how the EOC works; we can use the pandemic exercise as an example
    - The first one we do will need to be well-scripted and organized (KISS – keep it simple)
- Again, volunteers were asked for; with no one volunteering, there was a motion to volunteer those who were not in the room so Shane Ludwig from the Utilities Board was freely volunteered by his co-worker. (Shane we look forward to see you at our first meeting)

TGB (Technology Governance Board)

- At the last TGB meeting 3 standards were approved
- The standards are expected to be implemented by the end of 2007
- Unless funding is available before the end of 2007, all laptops with confidential information will need to be encrypted by the end of the calendar year 2007
- The TGB requested that DAS submit a formal request for funding; it may be difficult to submit for this session. The ISO will ask the TGB for how they would like to proceed; appears the only way at this point to get money for funding for this is through the Tech funding; this will affect others who are counting on dollars from the Tech funding and those agencies will need to be notified
- All removable media must be encrypted if it contains confidential information by the end of the calendar year. At this point, there is no way to enforce unless additional tools become available. Again, this is a funding issue
- The TGB decided that this was an area that was too important not to address; their consensus was that everything should be encrypted but it came down to

balance; it may hurt some agencies, but this is too important an issue to not address

- Because of a caveat in the previous two standards, there are ways for agencies to show how their data is classified. By August 2007 all agencies will be required to classify all data as either public or confidential. Some agencies have more classifications than this. It is important to understand agencies have to meet the minimum requirement, which is public or confidential. There was a question with regard to the framework for classifying the data. Security CIO reiterated that they have a commitment to assist agencies with the data; however, it is ultimately the agencies responsibility to classify the data
- Next question was "Who is the keeper of the information"? Answer: Agencies are required to classify the data and if requested will need to produce written documentation identifying their data classification
- With regard to the TGB requirements now in place, ie encryption, critical assets, etc. – if there are no dollars for encryption, how do we know that the data is encrypted; how do we know that all of the data is secure?
- Answer: That is all part of the trust with agencies; sometime a Memorandum of Understanding (MOU) between the agencies will need to be developed. Part of that MOU should be how data are managed and secured. In the case of DHS, there are civil and criminal penalties. As a whole, there has been a change in the past 3-5 years in business practices with regard to securing data. Even if some agencies have already documented this, the ISO office may be able to assist with a template so other agencies can get started. The standards are now on the ITE web page. http://das.ite.iowa.gov/standards/enterprise_it/index.html
- If there are things that need to be posted to the state security site, ie best practices, templates, etc. staff can work with Bill Hubbard. The ISO office is trying to get the Iowa interactive site posted. At this point, it is being postponed to the end of January.
- Homeland Security cannot get to the ITE website because they are behind the state firewall. This issue is going to be worked to try to develop ways for Homeland Security to access the intranet. Appears that most other agencies can get to the site

Enterprise Connectivity Standards

- Last month CIO Security Council discussed the first draft written by a consultant called Interconnectivity Standards. It represents minimum security standards for all state agencies connected to the enterprise network.
- Some agencies do not own their networking operations. Nevertheless, they are still responsible for ensuring their network is secure
- This may require a formal agreement between the agency and their service provider
- If connectivity to the shared network is with a third party, that link needs to meet these requirements as well

- The state has the right to assess compliance with an agency and a third party to see if it is meeting the enterprise connectivity standards
- **Firewalls –**
    - they need to be configured to deny all and then open to individual ports; documentation needs to show why ports were opened
    - important to establish a DMZ and create further segregation, when necessary
    - Wording of the language in the standard does affect the enforceability. “Where possible” is not preferred language but in some instances may be necessary
    - For now the focus will be on perimeter firewall requirements
- **Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)**
    - The requirement is to watch the traffic so agencies can see what is getting through the firewall
    - Ideally it would be good if agencies could share what kind of traffic they are seeing coming through
    - Currently only a few agencies have an IDS or IPS in place.
    - From an incident response perspective it is helpful to have the IDS/IPS logs
    - What is the cost? The real cost is the body to manage and watch it. Many responded that it will be at least a ½ time FTE if not more. Again, the cost of this came up and how agencies are going to be able to pay for this and manage it
    - Dept of Revenue indicated they would feel better if the ISO could identify which agencies currently have the IDS/IPS and how they are monitoring traffic
- **Auditing** – agencies currently need to turn on logging for what kinds of things are passing through their network. Currently the requirement is that 6 months’ logs will be required. Some commented they feel that 6 months of logs are not long enough to keep the logs. Some also noted that agencies are required to keep logs for a period of time that is consistent with the agency regulations which could be different for each agency as they have different governing bodies
- **Identification Authorization** – all agreed this is fine
- **Logical Access Controls –** logon banners are required.
- **AntiVirus** –
    - Need to have a documented response plan if there is a virus incident
    - Discussed the variance that is available to state agencies if for some reason they do not feel that they need AntiVirus on a particular server. Although most agreed that this is not a good practice, there are situations where a variance can be requested through the State Information Security Office. The language now is that the variance has to be reviewed every six months and reapproved. Based on need, this may change.
- **VPN** – Encryption is required. Members will need to review and follow-up with comments to the ISO

- **ISO will be asking for feedback regarding this proposed new standard**. Changes will be made, based upon feedback received, and the revised policy will be sent out to agencies representatives for additional comment prior to sending to the TGB. Would like to send this policy to the TGB by the end of January
- **Standards** - the only standards that have been passed by the TGB are those that have already been identified.
- **Operational Security Testing – Greg will make the changes**
- **Training and Awareness –** applies to all staff
- **Security Reviews –** yearly audits/assessments are required
- **Reporting –** members indicated it would be better to report incidents, etc to one person, meaning the ISO, rather than to each other
- **Disconnect –** what would trigger a disconnection? What steps need to be taken before an agency can be disconnected? The ISO will create a draft with more specifics and make available for other members to review. One question: Does the ICN have the ability to disconnect? If so, what is their policy? Also, the definition of a security incident is open to broad interpretation. Can it be modified?
- **MISC –** Bill Hubbard made copies of the presentation from the Cyber Security Conference available to all attendees

Next meeting is scheduled for February 14, 2007 – Someone needs to bring treats!